Pearson BTEC Level 3 Nationals Diploma, Extended Diploma

Window for supervised period:
Tuesday 11 January 2022 – Monday 31 January 2022

Supervised hours 4 hours

Paper reference **20158K**

Information Technology

UNIT 11: Cyber Security and Incident Management

Part B

You must have:
Forensic_Analysis.rtf

Instructions

- **Part A** and **Part B** contain material for the completion of the set tasks under supervised conditions.
- There are 43 marks for **Part A** and 37 marks for **Part B**, giving a total mark for the set tasks of 80.
- **Part A** and **Part B** are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.
- This booklet should be kept securely until the start of the 4-hour, **Part B** supervised assessment period.
- **Part A** will need to have been completed and kept securely before starting **Part B**.
- Both parts will need to be completed during the 3-week period timetabled by Pearson.
- **Part A** and **Part B** tasks must be submitted together for each learner.
- **Part A** materials must not be accessed during the completion of **Part B**.
- This booklet should not be returned to Pearson.
- Answer **all** activities.

Information

- The total mark for this Part is 37.

Turn over ▶

Pearson

Instructions to Invigilators

This paper must be read in conjunction with the unit information in the specification and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document. See the Pearson website for details.

Refer carefully to the instructions in this task booklet and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document to ensure that the assessment is supervised correctly.

Part A and **Part B** set tasks should be completed during the period of 3 weeks timetabled by Pearson. **Part A** must be completed before starting **Part B**.

The 4-hour **Part B** set task must be carried out under supervised conditions.

The set task can be undertaken in more than one supervised session.

An electronic template for activity 4 is available on the website for centres to download for learner use.

Learners must complete this task on a computer using the templates provided and appropriate software. All work must be saved as PDF documents for submission.

Invigilators may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Invigilators should note that they are responsible for maintaining security and for reporting issues to Pearson.

Maintaining Security

- Learners must not bring anything into the supervised environment or take anything out.
- Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.
- Internet access is not permitted.
- Learner's work must be regularly backed up. Learners should save their work to their folder using the naming instructions indicated in each activity.
- During any permitted break, and at the end of the session, materials must be kept securely and no items removed from the supervised environment.
- Learners can only access their work under supervision.
- User areas must only be accessible to the individual learners and to named members of staff.
- Any materials being used by learners must be collected in at the end of each session, stored securely and handed back at the beginning of the next session.
- Following completion of **Part B** of the set task, all materials must be retained securely for submission to Pearson.
- **Part A** materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

Each learner must create a folder to submit their work. Each folder should be named according to the following naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11B

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11B

Each learner will need to submit 2 PDF documents, within their folder, using the file names listed.

Activity 4: activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]

Activity 5: activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]

An authentication sheet must be completed by each learner and submitted with the final outcomes.

The work should be submitted no later than 2 February 2022.

Instructions for Learners

Read the set task information carefully.

Plan your time carefully to allow for the preparation and completion of all the activities.

Your centre will advise you of the timing for the supervised period. It is likely that you will be given more than one timetabled session to complete these tasks.

Internet access is not allowed.

You will complete this set task under supervision and your work will be kept securely at all times.

You must work independently throughout the supervised assessment period and must not share your work with other learners.

Your invigilator may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Part A materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

You must create a folder to submit your work. The folder should be named according to the following naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11B

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11B

You will need to submit 2 PDF documents, within your folder, using the file names listed.

Activity 4: activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]

Activity 5: activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]

You must complete an authentication sheet before you hand your work into your invigilator.

Set Task Brief

Hotela Ĉeno

Reganta Virino is the Chief Executive of Hotela Ĉeno (HC), a hotel chain on the island of Varma Loko. The hotels are rated as four star and HC gets most of its business from the tourist trade. This includes block bookings for package tours by international holiday companies and individual bookings by independent travellers.

Reganta has many years of management experience in the hotel business but regards herself as an IT user rather than an IT specialist.

Client brief

You advised Reganta on cyber security matters for a hotel near Varma Loko Airport. When you gave her your Management Report she asked you to review the investigation of a recent cyber security incident at another hotel.

The incident occurred last Friday, the 7th January, at Hotelo Aliloke in Marabordo, a popular seaside resort. HC provides an app for its guests that gives information about Varma Loko. The app also displays adverts for tourist attractions, with links that allow guests to purchase tickets.

On Friday morning a guest complained to reception that the HC app was showing an advert for a casino. She said that she didn't think the advert was appropriate for her children. The receptionist realised that the advert was not one of their standard adverts and passed the complaint on to the Hotel Manager.

Evidence items from the security incident at Hotelo Aliloke

Evidence items include:

1. Hotel Manager's account
2. IT Manager's report
3. High level design for the app
4. Network diagram
5. Floor plan and switch setup in the Teens' Club
6. Cyber security document – incident management policy.

1 Hotel Manager's account

On Friday morning a receptionist asked me to talk to a guest. The guest was unhappy about an advert for a casino which appeared on the app.

The guest showed me her tablet with the advert displayed. The advert was definitely not one of ours. We used the app for a few minutes to see if anything else suspicious appeared. There was nothing and the advert did not repeat.

That sort of thing often happens. Usually it's a bit of malware on the guest's computer and we offer to do a scan-and-fix for them. That usually works, but I'd had two similar reports earlier that morning, so I was a little concerned about the situation. I asked the guest to visit the IT centre with me.

I introduced her to one of our technicians, and left them looking at the tablet while I talked to Estro, the IT Manager.

Estro's team had been working on the previous reports and discovered some items of interest. I asked him to log the three reports as a single incident.

While we were talking another report came in saying the advert had appeared on a console in our Teens' Club **(see evidence item 5).** Estro and I agreed that the adverts should be suspended. It's just a bit of server-side script so Estro simply commented it out.

2 IT Manager’s report

Date: Saturday 8/1/2022

Author: Estro Cifereca

IT Manager, Hotelo Aliloke

Preamble
This report covers the investigation into the display of a rogue advert. The investigation turned up some suggestive information but was inconclusive. The guests involved were all on the same package tour and had to fly home to America that day. This meant we were time limited in examining guests’ devices.

Laptop 1 & Tablet 1
Friday 09:30 A guest approached an IT technician and reported that the HC app was showing an advert for a casino. He complained it could not be clicked like the rest of the adverts.

The guest had a laptop, running Windows 10, and the technician told the guest that it may have a malware problem. She logged the event and offered to perform a scan-and-fix. This is standard practice. It keeps guests happy and often solves the problem.

09:47 While the scan was running, a second guest came to the IT centre with the same problem. This time on an Android tablet. This called the virus idea into question and the technician started looking at other factors.

She noticed that both machines were running the same browser and looked for add-ons that might be causing the problem. Both machines had a browser helper object (BHO) that our software flagged as suspicious. Further investigation showed it to be part of a popular American shopping app.

She offered to remove the BHO but both guests said that they used the shopping app frequently and it had not displayed unexpected adverts in the past.

Tablet 2
10:02 A third machine, also a tablet running Android, was brought in. The symptoms were exactly the same and the guest was also from America. I wanted to see if the machine had the same browser setup as the others.

Before I could start, a message arrived saying that the same advert had appeared on a console in our Teens’ Club. The consoles are powered by PCs running Linux. I suggested that we suspend the adverts until we had solved the problem. The Hotel Manager agreed and I stopped the script. The problems were then grouped as a single incident.

Guest data had probably not been compromised but it was possible so Hotela Ĉeno HQ was informed.

On investigation, Tablet 2 did have the same BHO. The guest agreed with the others that the shopping app was safe and that it usually displayed relevant consumer goods.

Page 1

Hotela Ĉeno app
We looked at the app and the advertising script **(see evidence item 3)**, but did not find the source of the rogue advert.

Ad rotator script
The app runs a simple script that selects random entries from a list of sources.

The hotel's adverts are held in a text file. e.g.

```
<a href=”http://www.HoteloAliloke.vl/click-21” target=”_top” >
<img src=”http://www.HoteloAliloke.vl/image-21” width=”468” height=”100”
alt=”Hotel Aliloke gala night” border=”0”></a>
```

All the Hotelo Aliloke sources were checked and nothing unusual was found. We did find one odd entry at the bottom of the list.

```
<a href=”https://googledrive.com/host/0B4fk8L7brt_ea3okeEFxWjJvWWM /click-1”
target=”_top” >
<img src=”https://googledrive.com/host/0B4fk8L7brt_ea3okeEFxWjJvWWM /image-
1” width=”468” height=”100” alt=”Testing” border=”0”></a>
```

We tried the URL but got a 404 message. It's probably something left by the app developer.

Teens' Club
The consoles showed no signs of tampering and can only access the app via the internet. We did not find the BHO on the consoles. We did find some irregularities in the associated network wiring but there was no obvious link to the problem **(see evidence item 5).**

We altered the script to change adverts every second and restarted it late on Friday night. We spent several working hours on the consoles looking for the advert appearing but saw nothing. We did not find anything when scanning the console PCs.

Conclusions
Inconclusive, there were no further reports and we were unable to spend any more time with the guests' devices.

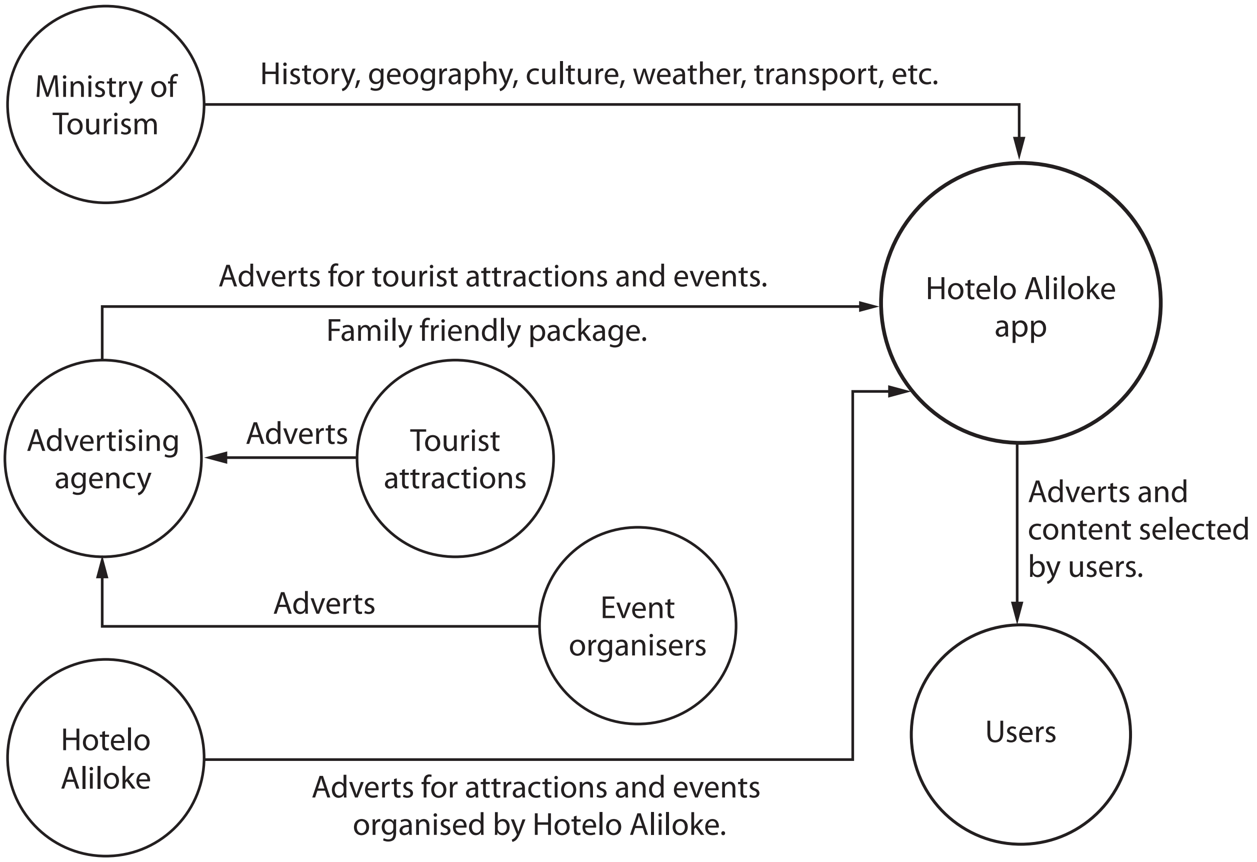
Possibilities from most to least likely:

- the advertising agency that supplies some of the adverts made a mistake or was compromised
- a mistake or compromise on an attraction site that supplies adverts to the agency
- a practical joke by someone in the hotel using our own system
- an external hack of our system.

23:59 The Incident was closed.

Page 2

3 High level design for the HC app


Ministry of Tourism
History, geography, culture, weather, transport, etc.
Hotelo Aliloke app
Adverts for tourist attractions and events.
Family friendly package.
Advertising agency
Adverts
Tourist attractions
Adverts and content selected by users.
Adverts
Event organisers
Hotelo Aliloke
Users
Adverts for attractions and events organised by Hotelo Aliloke.

The adverts are served by a script running on the hotel app server.

The Ministry does not supply adverts but may impose advert-like notices e.g. weather warnings.

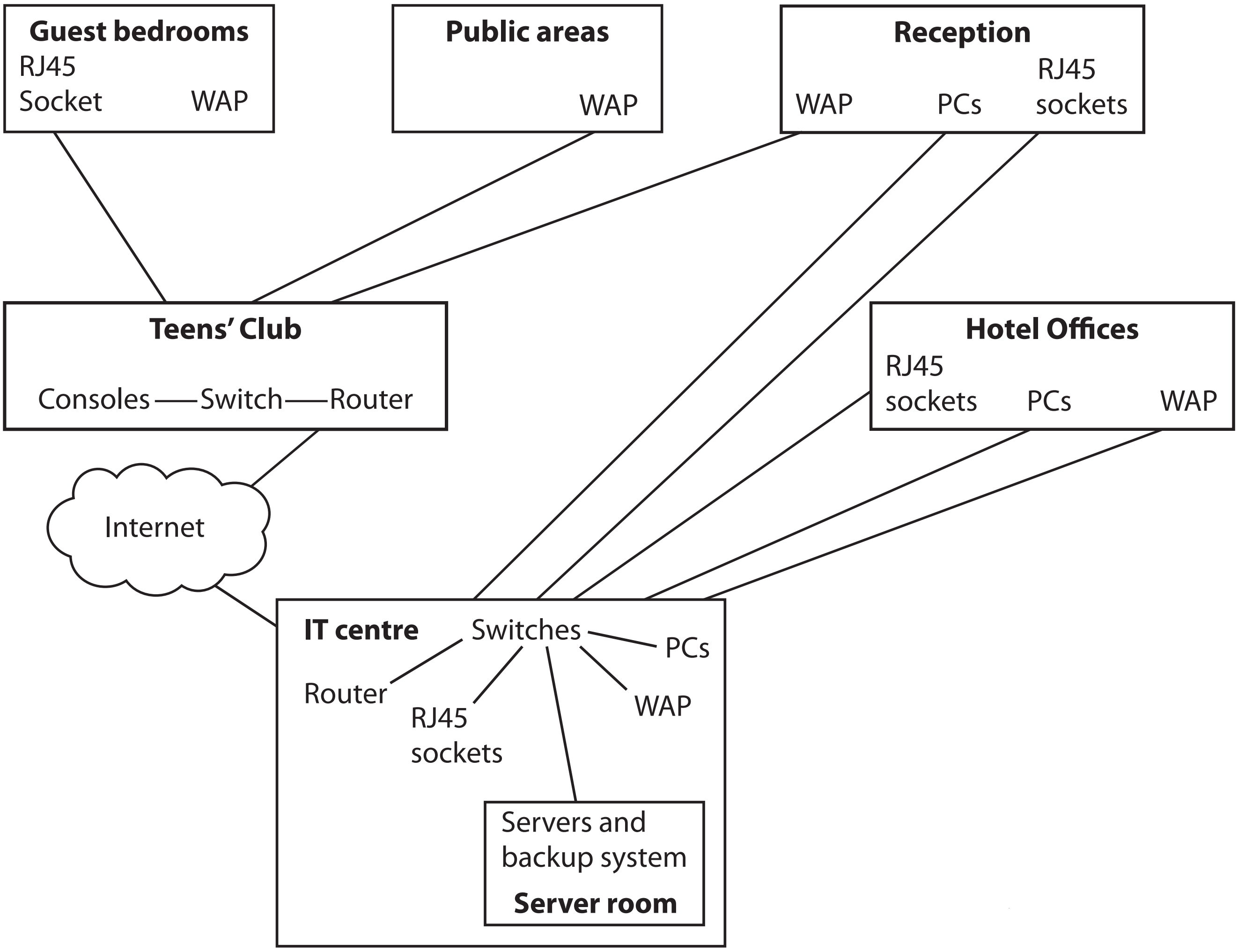
The advertising agency supplies adverts to the Hotela Ĉeno chain. Hotelo Aliloke has selected the family-friendly package.

Hotelo Aliloke supplies its own adverts for attractions and events organised by the hotel.

If a user clicks on an advert they will be taken to a web page containing further information. This page may be on the hotel's system or accessed via the internet.

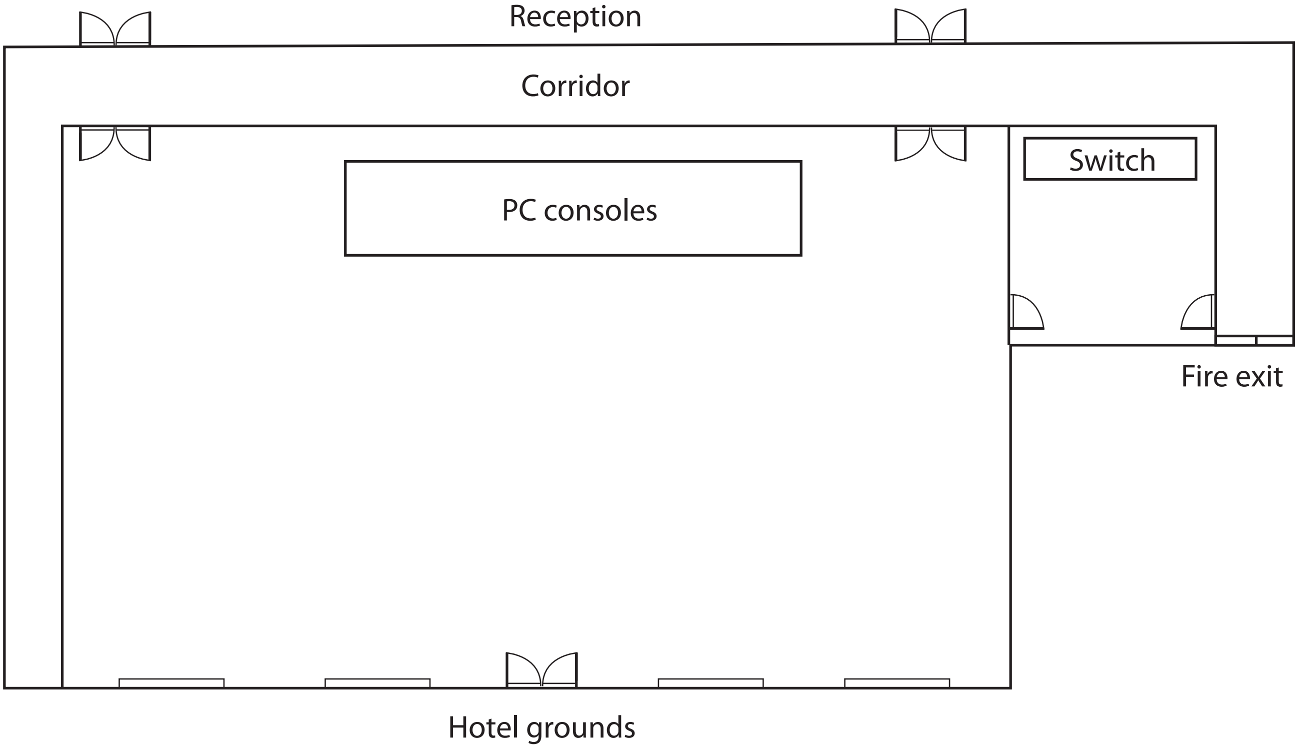
4 Network diagram

A conceptual diagram of the Hotelo Aliloke network.



5 Floor plan and switch setup in Teens' Club

Notes from Estro Cifereca, IT Manager.



Hotelo Aliloke was a conference centre before being converted to a hotel. The Teens' Club was the IT centre.

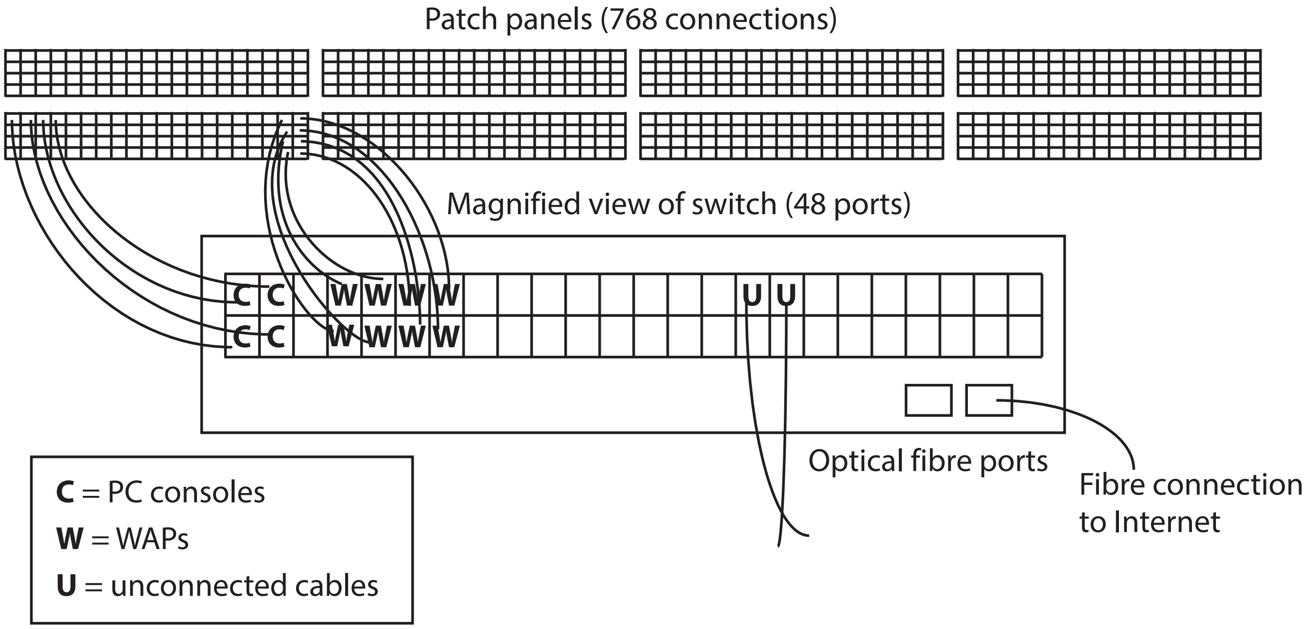
The consoles are touch screens for concealed PCs. There are no ports or connections available to guests. The consoles provide selected games, music, filtered web access, and the HC app. The PCs are networked by Ethernet. They do not have WiFi and are not linked to the main hotel system.

There is a small room at the top right of the plan. This was the switch room and still retains a 48 port switch and patch panels for the original cabling. There is also a router/DHCP server that gives a fibre internet connection.

The switch room is mainly used by the cleaners to store equipment. The doors from the Teens' Club and the corridor have mechanical push-button locks with a three digit code.

The switch is used to connect the hotel's free WAPs to the internet. The patch panels still connect to guest bedrooms. Guests who don't have a WiFi capable device can ask for a cable connection. That is quite rare and we just make a manual connection when needed. There were no connections on Friday.

Someone had left some unconnected cables hanging from the switch. These should have been put away. I've made a sketch of the setup.


Patch panels (768 connections)
Magnified view of switch (48 ports)
C C W W W W
C C W W W W
U U
Optical fibre ports
Fibre connection to Internet
C = PC consoles
W = WAPs
U = unconnected cables

6 Cyber security document – incident management policy

Incident management team

The team shall consist of:

- the Hotelo Aliloke IT Manager (team leader)
- the senior IT technician on site (deputy team leader)
- the technician who first responded to the incident
- personnel co-opted by the team leader as needed.

Incident reporting

Any member of staff who considers that an IT-related security incident has occurred must report it as soon as possible to the Computer Security Incident Response Team (CSIRT) leader.

Initially it may be reported verbally but this must be followed up by an email. It is the responsibility of the CSIRT to maintain detailed documentation on the incident from first report to final resolution.

Security incidents may include:

- theft of IT equipment
- theft of company data
- unauthorised access to Hotelo Aliloke IT systems
- infection of Hotelo Aliloke IT systems with malware.

Incident response procedures

(a) **Theft of IT equipment**

- Theft of IT equipment is a very serious issue. Any thefts must be reported at once to the CSIRT leader, initially a verbal report must be made followed up by email, providing as much information as possible (location and type of equipment, when it was last seen, etc.).
- CSIRT leader must ascertain if the item has actually been stolen (or if it is just missing).

- If the item is confirmed as stolen, CSIRT leader must inform the police and contact the finance department so they can inform insurers.
- CSIRT must prepare a report on the theft to the Hotelo Aliloke Hotel Manager and if needed justify the finances required to replace the stolen item.
- Where guest data may have been compromised, the incident must be reported to the Hotelo Aliloke Hotel Manager and Hotela Ĉeno HQ.

(b) **Theft of company data**

- Theft or loss of company data equipment may occur in a number of different ways.
- Any loss of company data must be reported at once to CSIRT leader, initially a verbal report must be made followed up by email.
- The CSIRT must investigate the loss and identify exactly what data has been lost or stolen and when the incident occurred.
- Having identified what has been lost or stolen and when, the CSIRT must retrieve backups and restore the data as soon as possible.
- The CSIRT should review the incident and implement procedures to prevent future losses.
- Where guest data may have been compromised, the incident must be reported to the Hotelo Aliloke Hotel Manager and Hotela Ĉeno HQ.

(c) **Infection of hotel IT systems with malware**

- Any member of staff who suspects that any IT system has been infected with malware must report it at once to the CSIRT leader, initially a verbal report must be made followed up by email.
- The infected system should be shut down as soon as possible.
- The CSIRT will investigate the infection and take appropriate measures to resolve the infection and restore the system.
- Where guest data may have been compromised, the incident must be reported to the Hotelo Aliloke Hotel Manager and Hotela Ĉeno HQ.
- Where a guest's device(s) are suspected of being a source of malware, an offer must be made to perform a scan-and-fix. Where guests decline the service the device(s) must be blacklisted.

(d) **Unauthorised access to hotel systems**

- Any member of staff who suspects that there has been unauthorised access to any Hotelo Aliloke IT system must report it at once to the CSIRT leader, providing as much detail as possible (which system, how access was obtained). Initially a verbal report must be made, followed up by email.
- The CSIRT will thoroughly investigate the incident and identify how the unauthorised access was obtained.
- The CSIRT will recommend action to prevent future occurrences (e.g. change passwords).
- Where guest data may have been compromised, the incident must be reported to the Hotelo Aliloke Hotel Manager and Hotela Ĉeno HQ.

Part B Set Task

You must complete ALL activities within the set task.

Produce your documents using a computer.

Save your documents in your folder ready for submission using the formats and naming conventions indicated.

Read the set task brief carefully before you begin and note that reading time is included in the overall assessment time.

You have been advising Reganta Virino on cyber security. Now she has asked you to review the investigation of a cyber security incident.

Activity 4: Forensic incident analysis

Analyse the forensic evidence, including how the evidence was obtained, for the cyber security incident at Hotelo Aliloke.

Consider possible causes of the incident and come to a conclusion about the most likely cause of the incident.

Refer to evidence items 1–5 inclusive.

Produce a forensic incident analysis using the template **Forensic_Analysis.rtf**

Save your completed forensic incident analysis as a PDF in your folder for submission as **activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity.

(Total for Activity 4 = 14 marks)

Activity 5: Security report

Review the incident. Suggest improvements and explain how they would prevent a similar incident in the future.

Areas for improvement are:

- adherence to forensic procedures
- the forensic procedure and current security protection measures
- the security documentation.

Read the set task brief and evidence items 1–6 inclusive when answering the question.

Save your completed security report as a PDF in your folder for submission as **activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity.

(Total for Activity 5 = 20 marks)

TOTAL FOR TECHNICAL LANGUAGE IN PART B = 3 MARKS
TOTAL FOR PART B = 37 MARKS